General Data Protection Regulation and Confidentiality

Updated June 2020
Next Reviewed June 2022
Intermittent Changes will be agreed on an ad hoc basis due to new law and amendments

Data Protection and Confidentiality

Contents

1. Introduction

Inclusion North needs to collect and use information about individuals.

These can include volunteers, customers, suppliers, business contacts, employees and other people the organisation has a relationship with.

This policy describes how this personal data must be collected, handled, and stored to meet general data protection regulation standards

A separate policy is available for employee data. The Staff General Data Regulation Policy.

2. General Data Protection Regulation Law

The EU General Data Protection Regulation (UK compliance 2018) amended from The Data Protection Act (1998). The General Data Protection Regulation regulates how personal data is stored and handled and protects people from organisations misusing it. The aim of the GDPR is to protect all European citizens from misuse of data and to maintain privacy.

The new regulations are very complicated. It is extra legislation on top of the existing law. Inclusion North is fully committed to complying with the new regulations and any section in this policy will be corrected to meet the new regulations if they are found to be incorrect.

2.1 What this means for Inclusion North

This means that any data we hold or store on individuals is relevant to our business and is kept for a specific purpose and use.

The data must be kept secure and not shared with third parties without permission of the individual or organisation.

The Act provides stronger protection for sensitive personal information about ethnic origins, political opinions, religious beliefs, trade union membership, health, sexual life, and any criminal history.

The Act, with some exceptions, gives the right to find out what information is held by organisations. On written request, individuals are entitled to be supplied with an electronic copy of all the information an organisation holds about them.

3. Policy Scope

This Policy applies to all employees, volunteers, contractors, suppliers, and other people working on behalf of Inclusion North. In this policy we will refer to this group as ‘staff’.

It applies to all data that the company holds about individuals who could be identified.

This may include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Marketing preferences
- Courses attended

- Details of any contractual obligations
- Work history for volunteers
- Any data that identifies an individual
- Any other information relating to individuals

4. Responsibilities

Everyone who works for or with Inclusion North has some responsibility for making sure data is collected, stored, and handled correctly.

The Board of Directors is ultimately responsible for ensuring that Inclusion North meets its legal obligations.

The Chief Executive and Office Manager are responsible for:

- Keeping the Board updated about General Data Protection Regulations responsibilities, risks, and issues
- Reviewing the General Data Protection Regulation Policy annually
- Handling General Data Protection Regulation questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Inclusion North holds about them. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is working properly
- Approving any General Data Protection Regulation statements attached to letters and emails
- Working with other staff to make sure marketing items comply with General Data Protection Regulation Law.

- Obtaining permission and advising the people we hold data about; telling them what information is held, why it is held and what we will do with the data.

5. Staff Guidelines for Data Storage

The only staff able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is needed staff whose access to this is restricted can ask for it from their line manager.

Inclusion North will provide training to all staff to help them understand their responsibilities when handling data via an online training portal.

Staff must keep all data secure.

Strong passwords must be used, and they should not be shared.

Personal data should not be given to unauthorised people either within Inclusion North or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If it is no longer required, it should be deleted or disposed of securely.

Staff should request help from their line manager or the office manager if they are unsure about any aspect of General Data Protection Regulations.

6. Data Storage and Removal

6.1 Paper

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.

When not being used, papers or files should be kept in a locked drawer or filing cabinet.

Staff should make sure papers are not left where other people could see them e.g. on a printer.

Data printouts should be shredded and disposed of when no longer needed.

6.2 Electronic Data

Personal, identifiable data must not be stored on USB sticks. The exception is archived information prior to May 18 being held on an external hard drive, locked in the Inclusion North office.

All computers or other storage devices and mobile phones must be password protected. Computers purchased after February 2018 will include TCG Encryption and Windows Professional software.

Data is backed up in the cloud with Office 365.

Data must never be saved directly to laptops, tablets, or phones.

All servers and computers containing data must be protected by approved security software and a firewall.

Access to the Inclusion North 365 account will be restricted to employees and will be protected by a password. Individual Folders to be shared to facilitate joint working will be done via

WeTransfer or an individual Dropbox and will not contain identifiable information.

Share Point must not be downloaded onto any laptop, PC, tablet, or phone that does not belong to Inclusion North.

Any Inclusion North devices which are no longer needed will be securely disposed of. Hard drives will always be wiped clean of data prior to disposal.

Share Point must only be downloaded onto Inclusion North devices that have a password for opening/starting them.

Documents which include sensitive or personal information will be kept in relevant files.

Staff will have access to information they need to do their job, not all identifiable data.

Identifiable data that are Contact Lists, or Photos will be stored in a central file to ensure it can be found and disposed of when required.

6.3 Removal and Destroying Identifiable Data

Identifiable Data will be held by Inclusion North for 5 years, after it is no longer used for the purpose it was collected, unless the person whose data it is asks to have it removed. A record of removal will be kept for the purpose of evidence for the Information Commissioners Office.

Information is stored for 5 years for reference purposes for projects and work people may have been involved in or events people may have attended, enabling Inclusion North to keep people informed of relevant work and events.

Identifiable Data that is part of our financial procedures is kept for 6 years as this is a legal requirement of HMRC.

Identifiable Data will be deleted from computer files, and Email groups.

Identifiable Data in paper form will be shredded and disposed of.

7. Data Use

When working with personal data staff should make sure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally.

Personal data should not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Staff should not save copies of personal data to their own computers.

Passwords will be stored on a secure password protected document to ensure in emergencies access can be obtained.

8. Data Accuracy

To comply with the law Inclusion North must take reasonable steps to make sure data is kept accurate and up to date.

Data should be held in agreed folders in Share Point.

Data should be updated as soon as inaccuracies are discovered.

If staff think the data held about people or organisations is inaccurate they must correct it or delete it.

9. Right of Access Requests

Anyone whose personal data is held by Inclusion North may:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations
- Ask for all data to be removed, this is the right to be forgotten

A request for information like this is called ~~a~~ Right of Access Request. They will be given this information free of charge within one month of their request, unless the request is deemed to be excessive.

Inclusion North has the right to refuse to respond to repetitive, unreasonable, or excessive requests. They will be informed of why Inclusion North has refused to respond.

They have the right to inform the Information Commissioners Office if they receive a letter of refusal to respond within one month of the date of the letter.

The office manager will respond to any requests for data. The identity of anyone requesting data must be verified before any data is given.

10. Confidentiality

Inclusion North recognises that staff, get information about individuals and organisations through their work. In most cases such information will not be stated as confidential and staff may have to use common sense in identifying whether information is expected to be confidential. If in doubt staff should seek advice from their manager.

When asking for information staff should inform groups, organisations, or individuals why they are doing so. They should explain how the information will be used and stored. They should ask permission to keep and use this information.

Staff may share information with their Line Manager to discuss issues and seek advice. They will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial, or private without the knowledge or consent of the individual, or an officer, in the case of an organisation

Staff should avoid sharing personal information or comments (gossip) about individuals with whom they have a professional relationship.

Staff should avoid talking about organisations or individuals in social settings or on social media platforms.

There may be times where colleagues would want to discuss difficult situations with each other to help solve a problem.

If staff get information from individuals outside Inclusion North about the behaviour of a colleague, then this should be dealt with

sensitively. The appropriate colleague should tell the individual about the Complaint Procedure and advise them accordingly.

If staff are unhappy with the behaviour of a colleague and have sensitive information that could be evidenced through investigation, they should discuss it with the appropriate line manager under the Whistle Blowing Procedure. Any allegation, which is found to be malicious, or ill-founded, will be dealt with under the Disciplinary Procedure for staff and the Volunteer policy for Volunteers. If staff or people whose information we hold believe a customer, suppliers, business contact has broken confidentiality they need to report this to the Office Manager or Chief Executive for investigation and possible reporting to the Information Commissioners Office.

Where there is a legal duty on Inclusion North to disclose information, the person that is affected will be informed that disclosure has or will be made.

Where information is sensitive it should be clearly labelled 'Confidential.' Records should be kept in a locked cabinet and any electronic records must be subject to the password of the Chief Executive.

Colleagues will not withhold information from their line manager unless it is purely personal to them and not business related.

When photocopying or working on confidential documents, staff must ensure they are not seen by people in passing. This also applies to information on computer screens.

Ensure confidential documentation or personal data is shredded before putting in the recycling bins.

10.1 Duty to disclose information

Inclusion North has a legal duty to disclose some information including:

- Child abuse will be reported to the Children's Services / Social Services Department

- Abuse of Vulnerable Adults should be reported to Adult Safeguarding

- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

In addition, staff believing an illegal act has taken place or that a person is at risk of harming themselves or others, must follow safeguarding policy.

Inclusion North should inform the person to whom this refers that the disclosure has been made.

10.2. Breach of Confidentiality of Data we hold

If persons whom Inclusion North hold data about, believe there has been a breach of confidentiality of the General Data Protection Regulation, they can raise a right to access request.

They can request that Inclusion North tells them how they have used their information and how Inclusion North has followed the Data Protection Act and GDPR principles.

If the person still has concerns about how Inclusion North has used their information they can contact the Information Commissioners Office Telephone: 0303 123 1113.

10.3 Whistleblowing

Anyone who has concerns about the use of Inclusion North funds, or any practice by any employee must comply with the requirements of the Whistle Blowing Policy.